

Building Cyber Resilient Enterprise

LTIMindtree Cyber Security Services Overview
- An introduction to Webster Bank

September 2025

LTIMindtree Cybersecurity Services Overview



4,042+

Security Experts



260+

Global Clientele



9

Cyber Defense Resiliency Centers



30+

IPs & Accelerators



8

Strategic Alliances Working with 200+ OEMs



Product Challenger in Cybersecurity Ecosystem 2024



Major Contenders in Cybersecurity Services PEAK Matrix Assessment 2024



Disruptor in Cybersecurity Services 2025 RadarView



Brings comprehensive approach for transforming cybersecurity



Risk focused - Resiliency driven



Platform Powered



Gen AI enabled



Security transformation specialist



End to end coverage across 8 security domains



Best-of-breed Alliances



CoE-driven services - accelerators playbooks, templates, frameworks

Verticals

- Banking & Financial Services
- Insurance
- Hi Tech
- Energy and Utilities
- Manufacturing
- Healthcare and Life Sciences
- Communications, Media, and Entertainment
- Retail & CPG
- Travel, Transport, and Hospitality

Cyber Security Service Catalogue

Cyber Defense Service

Managed Extended Detection and Response (MxDR)

- 24x7 AI driven Incident Response
- Security Platform Management
- Threat Intelligence
- Use Case Management
- Forensics and Incident Response
- Threat Exposure Management
- Threat Hunting
- Attack Surface Management
- Managed EDR & Email Security

Cloud & Infra Security

- CNAPP, CSPM
- Network Security
- Digital Workplace Security
- Gateway Security
- Zero Trust , SASE, SDN
- Vulnerability Management
- Penetration testing
- Red Teaming
- Breach Attack Simulation

IoT / OT Security

- IT/OT SOC
- Advanced IT/OT Threat Intelligence
- OT Vulnerability Management
- Compliance and Risk Assessment
- Cyber Physical System Resilience

AI-Driven Enterprise Resilience

Global Delivery Framework

CDRC

Digital Trust

Identity Management

- Single Sign On , Multifactor Authentication
- Identity Governance & Administration
- Privilege Identity & Access Mgmt.

Data Security

- Data Discovery & Classification
- Data Loss Prevention
- Data Protection /Encryption
- Privacy Compliances
- Public Key Infrastructure (PKI)

Risk & Compliance

GRC

- Governance, Risk & Compliance Management
- Third Party Risk Management
- Security training & awareness
- Cyber Security Maturity Assessment
- Cyber Resiliency Services

Security Assessments

Application Security

- Static Application Security Testing
- Dynamic Application Security Testing
- Penetration Testing, Threat Modelling
- DevSecOps
- Securing AI/ LLM

Strategy & Consulting

Implementation & Transformation

Shared / Dedicated Managed Security Services

Monitoring

SLAs & KPIs

Secure AI Service Offerings

Services

-  AI Security Advisory

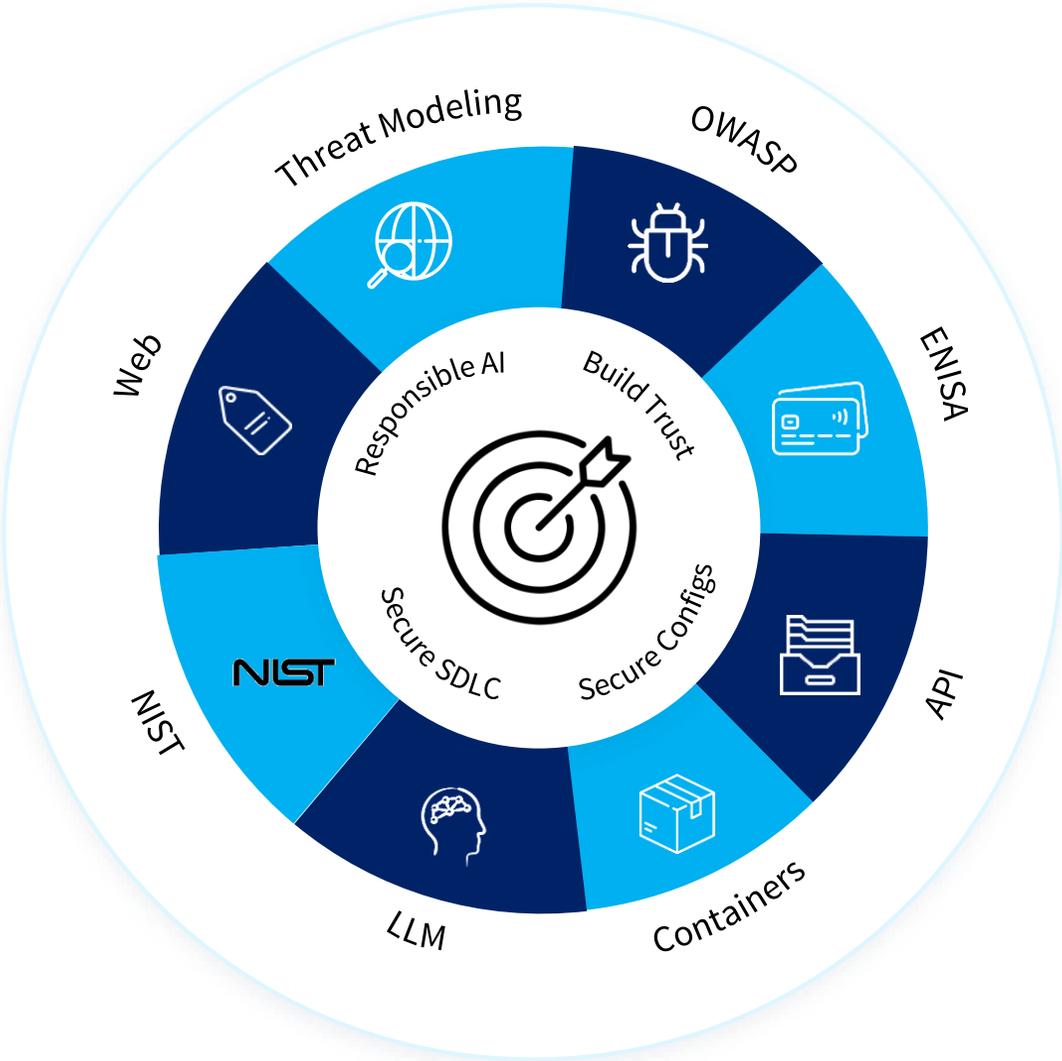
-  AI Monitoring & Observability

-  AI Security & Risk Assessment

-  AI Bill of Materials

-  AI Guardrails

-  AI Red Teaming



Value Propositions

-  Safeguard against threats to AI

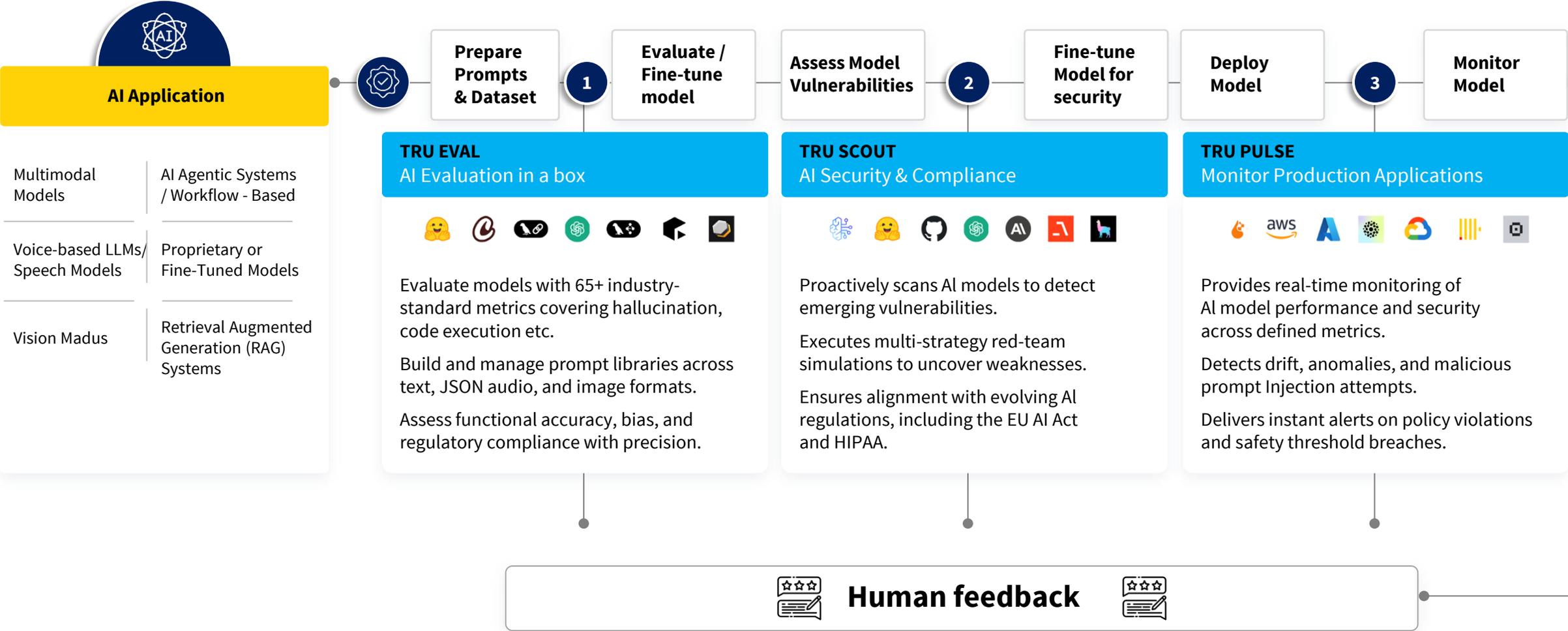
-  Scale AI applications securely

-  Adherence to responsible AI

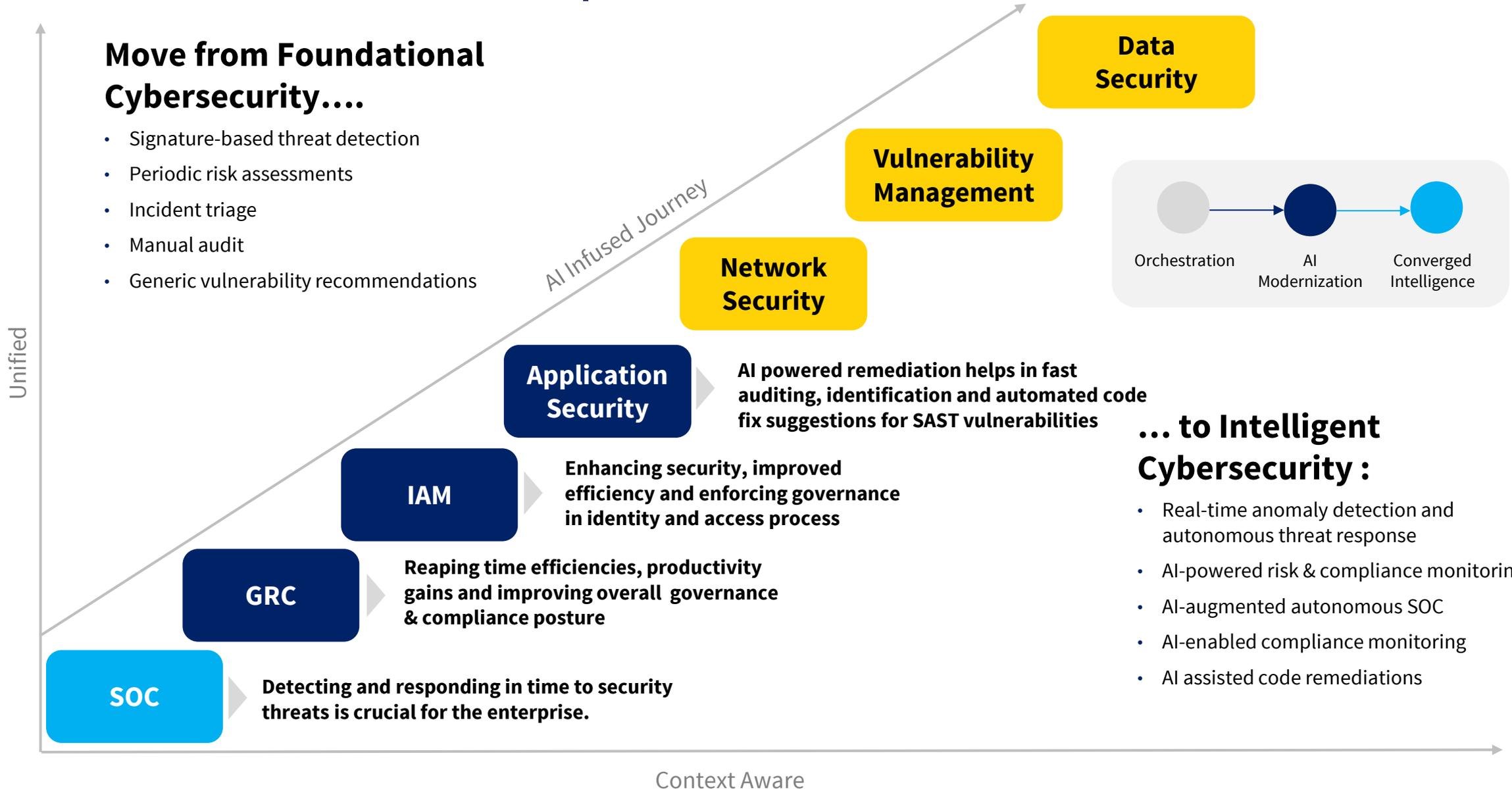
-  Industry standards compliance

-  Prevent sensitive data loss

In the BlueVerse, We build “Trust” using LTIM Trusys Platform



AI-Powered Transformation | CISO Office



SOC Security Services for a large private bank



Scope

The scope of the work includes Supporting SOC services

- SOC Analyst L1,L2 and L3 support services (24X7)
- Platform Management (9X5)
- Soc Governance Risk (9X5)
- Threat Hunting (9X5)
- Threat Intelligence (9X5)
- Management Information Systems MIS (9X5)



Volumetrics/ Key Takeaways

- Incident Count – ~12000+ Yearly
- EPS –7 to 10 lacs
- Log Sources – 270 plus
- Devices Integrated – 10K -12K
- 30 Engineers and Security SMEs deployed at Banks location for managing SOC operations 24X7



Key Challenges

As a trusted partner, we have a deep understanding of the client's SOC operations issues. The main challenges they encountered included:

- Lack of Automation
- Ticket / Incident closure comments issues
- High False positive alerts in SIEM solution.
- Regulatory and Compliance report challenges.
- End to End Process documentation.



Solution Proposed

- Prepared 500 plus IRC's (Incident response control) to automate Incident response tasks via Xsoar tool
- Identify use cases triggering maximum False positives and fine tune the same
- Carried out SOC Maturity assessment and came up with Observations / Areas of Improvement with relevant recommendations.
- Review of Incidents / Tickets to identify gaps / mistakes in closure comments.



Benefits

- Huge number of L1 tasks automated.
- Streamlined Regulatory and Compliance reports accuracy.
- Reduction in False positives due to Fine Tuning of use cases.
- Streamlined SOC operations post SOC Maturity assessment.

Reach out to us for more interesting conversations....



Abhayraj Deshmukh

Global Client Partner

Email - abhayraj.deshmukh@ltimindtree.com

Mob - +1 2146957941



Getting to the
future, faster.
Together.

with LTIM Cybersecurity